

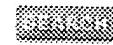
091608735

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	12917	705/60 or 380/277 or 380/259 or 380/281 or 713/156 or 713/176 or 713/200 or 713/201 or 283/13 or 705/75 or 382/276 or 382/308 or 705/71 or 713/171 or 380/279	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/04/26 18:56
L2	48	"digital signature" and "secret key" and indicium and distribut\$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/04/26 18:57
L3	24	1 and 2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/04/26 18:57
L4	19	pagel.inv. and martin	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/04/26 18:58


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
Search: The ACM Digital Library The Guide

US Patent & Trademark Office

postage and indicium and "digital signature" and "secret key"

**THE ACM DIGITAL LIBRARY**
 [Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used [postage](#) and [indictum](#) and [digital signature](#) and [secret key](#)

Found 342 of 153,034

Sort results
by
 Save results to a Binder[Try an Advanced Search](#)Display
results
 [Search Tips](#)Try this search in [The ACM Guide](#) Open results in a new window

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

1 [SPINS: security protocols for sensor networks](#)

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5

Full text available: [pdf\(213.37 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)



2 [Some facets of complexity theory and cryptography: A five-lecture tutorial](#)

Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Full text available: [pdf\(2.78 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)



3 [Secret key distribution protocol using public key cryptography](#)

Amit Parnerkar, Dennis Guster, Jayantha Herath
October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

Full text available: [pdf\(74.93 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



4 [Digital signature schemes for computer communication networks](#)

Henk Meijer, Selim Akl
October 1981 **ACM SIGCOMM Computer Communication Review , Proceedings of the seventh symposium on Data communications**, Volume 11 Issue 4

Full text available: [pdf\(338.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



5 [Session 8A: Lower bounds on the efficiency of encryption and digital signature schemes](#)

Rosario Gennaro, Yael Gertner, Jonathan Katz
June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing**

Full text available: [pdf\(236.93 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



6 [Verifiable encryption of digital signatures and applications](#)

Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Full text available: [pdf\(258.12 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



7 [ID-based secret-key cryptography](#)

Marc Joye, Sung-Ming Yen

October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4

Full text available:  pdf(513.15 KB) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

8 [Efficient verifiable encryption \(and fair exchange\) of digital signatures](#)

Giuseppe Ateniese

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available:  pdf(781.40 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

9 [An efficient protocol for unconditionally secure secret key exchange](#)

Michael J. Fischer, Rebecca N. Wright

January 1993 **Proceedings of the fourth annual ACM-SIAM Symposium on Discrete algorithms**

Full text available:  pdf(907.75 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

10 [Password Management and Digital Signatures: Twin signatures: an alternative to the hash-and-sign paradigm](#)

David Naccache, David Pointcheval, Jacques Stern

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available:  pdf(402.64 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

11 [Responses to NIST's proposal](#)

Ronald L. Rivest, Martin E. Hellman, John C. Anderson, John W. Lyons

July 1992 **Communications of the ACM**, Volume 35 Issue 7

Full text available:  pdf(8.06 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

12 [Simple forward-secure signatures from any signature scheme](#)

Hugo Krawczyk

November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**

Full text available:  pdf(231.13 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

13 [Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures](#)

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Full text available:  pdf(386.51 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

14 [How to sign given any trapdoor permutation](#)

Mihir Bellare, Silvio Micali

January 1992 **Journal of the ACM (JACM)**, Volume 39 Issue 1

Full text available:  pdf(1.39 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

15 [The digital signature standard](#)

CORPORATE NIST

July 1992 **Communications of the ACM**, Volume 35 Issue 7

Full text available:  pdf(3.12 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

16 Secure personal computing in an insecure network

Dorothy E. Denning

August 1979 **Communications of the ACM**, Volume 22 Issue 8Full text available: pdf(654.64 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)**17** Non-repudiation with mandatory proof of receipt

Tom Coffey, Puneet Saidha

January 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 1Full text available: pdf(707.87 KB) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)**18** On-line e-wallet system with decentralized credential keepers

Stig Frode Mjølsnes, Chunming Rong

February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1Full text available: pdf(240.23 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)**19** Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4Full text available: pdf(2.50 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)**20** Analysis and verification: Cryptographic tamper evidence

Gene Itkis

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**Full text available: pdf(256.12 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

Search Results[BROWSE](#)[SEARCH](#)[IEEE XPLOR GUIDE](#) [e-mail](#)

Results for "(master key'<in>metadata)"

Your search matched 19 of 1152881 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance in Descending** order.[» View Session History](#)[» New Search](#)[Modify Search](#)[» Key](#)

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[Select Article Information](#)

- (**master key'<in>metadata**)
- Check to search only within this results set
- Display Format: Citation Citation & Abstract
- 1. Cryptographic master-key-generation scheme and its application to public key distribution**
Kiesler, T.; Harn, L.;
Computers and Digital Techniques, IEE Proceedings E [see also Computers and Digital Techniques, IEE Proceedings-E]
Volume 139, Issue 3, May 1992 Page(s):203 - 206
[AbstractPlus](#) | Full Text: [PDF\(304 KB\)](#) IEEE JNL
- 2. Motion trajectory based video authentication**
Wei-Qi Yan; Kankanhalli, M.S.;
Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on
Volume 3, 25-28 May 2003 Page(s):III-810 - III-813 vol.3
[AbstractPlus](#) | Full Text: [PDF\(374 KB\)](#) IEEE CNF
- 3. Reducing radio energy consumption of key management protocols for wireless sensor networks**
Lai, B.-C.C.; Hwang, D.D.; Kim, S.P.; Verbauwhede, I.;
Low Power Electronics and Design, 2004. ISLPED '04. Proceedings of the 2004 International Symposium on
9-11 Aug. 2004 Page(s):351 - 356
[AbstractPlus](#) | Full Text: [PDF\(491 KB\)](#) IEEE CNF
- 4. A Simple Forward Secure Blind Signature Scheme Based on Master Keys and Blinding**
Yeu-Pong Lai; Chin-Chen Chang;
Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on
Volume 2, 25-30 March 2005 Page(s):139 - 144
[AbstractPlus](#) | Full Text: [PDF\(136 KB\)](#) IEEE CNF
- 5. Design of hierarchical keys for a multi-user-based watermarking system**
Feng-Hsing Wang; Jain, L.C.; Jeng-Shyang Pan;
Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on
Volume 2, 27-30 June 2004 Page(s):919 - 922 Vol.2
[AbstractPlus](#) | Full Text: [PDF\(568 KB\)](#) IEEE CNF
- 6. Secret sharing in graph-based prohibited structures**
Hung-Min Sun; Shiu-Pyng Shieh;
INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE
Volume 2, 7-11 April 1997 Page(s):718 - 724 vol.2

[AbstractPlus](#) | Full Text: [PDF\(484 KB\)](#) IEEE CNF

7. **Key management for decentralized computer network services**

Harn, L.; Hung-Yu Lin;
Communications, IEEE Transactions on
Volume 41, Issue 12, Dec. 1993 Page(s):1777 - 1779
[AbstractPlus](#) | Full Text: [PDF\(280 KB\)](#) IEEE JNL

8. **Managing secure communications with multilevel security and restricted character set translation**

Chyan Yang; Chien-Chao Tsai;
Selected Areas in Communications, IEEE Journal on
Volume 11, Issue 5, June 1993 Page(s):745 - 756
[AbstractPlus](#) | Full Text: [PDF\(1020 KB\)](#) IEEE JNL

9. **A study on secure wireless networks consisting of home appliances**

Nakakita, H.; Yamaguchi, K.; Hashimoto, M.; Saito, T.; Sakurai, M.;
Consumer Electronics, IEEE Transactions on
Volume 49, Issue 2, May 2003 Page(s):375 - 381
[AbstractPlus](#) | Full Text: [PDF\(510 KB\)](#) IEEE JNL

10. **Comments on the security of fast encryption algorithm for multimedia (FEA-M)**

Youssef, A.M.; Tavares, S.E.;
Consumer Electronics, IEEE Transactions on
Volume 49, Issue 1, Feb. 2003 Page(s):168 - 170
[AbstractPlus](#) | Full Text: [PDF\(322 KB\)](#) IEEE JNL

11. **An unbalanced key establishment scheme for heterogeneous wireless networks**

Huang, Q.; Kobayashi, H.; Liu, B.;
Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE
Volume 4, 29 Nov.-3 Dec. 2004 Page(s):2169 - 2174 Vol.4
[AbstractPlus](#) | Full Text: [PDF\(601 KB\)](#) IEEE CNF

12. **Multilevel security with restricted character set translation**

Yang, C.; Tsai, C.-C.;
Military Communications Conference, 1992. MILCOM '92, Conference Record. 'Command Fusing Command, Control and Intelligence', IEEE
11-14 Oct. 1992 Page(s):686 - 690 vol.2
[AbstractPlus](#) | Full Text: [PDF\(392 KB\)](#) IEEE CNF

13. **Control flow analysis in presence of exceptions for Java**

Yahyaoui, H.; Tawbi, N.; Rodrigue, J.-F.;
Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference
Volume 2, 4-7 May 2003 Page(s):1363 - 1368 vol.2
[AbstractPlus](#) | Full Text: [PDF\(462 KB\)](#) IEEE CNF

14. **Reducing Radio Energy Consumption of Key Management Protocols for Wireless Networks**

Bo-Cheng Charles Lai; Hwang, D.D.; Sungha Pete Kim; Verbauwhede, I.;
Low Power Electronics and Design, 2004. ISLPED '04. Proceedings of the 2004 International Symposium on
09-11 Aug. 2004 Page(s):351 - 356
[AbstractPlus](#) | Full Text: [PDF\(160 KB\)](#) IEEE CNF

15. **Identity-based threshold signature scheme from the bilinear pairings (extended abstract)**

Joonsang Baek; Yuliang Zheng;
Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on
20-23 June 2004 Page(s):103 - 107
[AbstractPlus](#) | Full Text: [PDF\(160 KB\)](#) IEEE CNF

Conference on
Volume 1, 5-7 April 2004 Page(s):124 - 128 Vol.1
[AbstractPlus](#) | Full Text: [PDF\(1363 KB\)](#) IEEE CFP

- 16. Intuition, perception, and secure communication**
Arazi, B.; Dinstein, I.; Kafri, O.;
Systems, Man and Cybernetics, IEEE Transactions on
Volume 19, Issue 5, Sept.-Oct. 1989 Page(s):1016 - 1020
[AbstractPlus](#) | Full Text: [PDF\(672 KB\)](#) IEEE JNL.

- 17. Cryptographic Authentication of Time-Invariant Quantities**
Lennon, R.; Matyas, S.; Meyer, C.;
Communications, IEEE Transactions on [legacy, pre - 1988]
Volume 29, Issue 6, Jun 1981 Page(s):773 - 777
[AbstractPlus](#) | Full Text: [PDF\(512 KB\)](#) IEEE JNL.

- 18. Security issues on B-ISDN billing system**
Chi-Chun Lo; Yi-Chun Yeh;
Network Operations and Management Symposium, 1998. NOMS 98., IEEE
Volume 1, 15-20 Feb. 1998 Page(s):287 vol.1
[AbstractPlus](#) | Full Text: [PDF\(40 KB\)](#) IEEE CFP

- 19. Design and implementation of smartcard-based secure e-mail communication**
Hsien-Hau Chen; Yung-Sheng Chen; Hsia-Ling Chiang; Chung-Huang Yang;
Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on
14-16 Oct. 2003 Page(s):225 - 231
[AbstractPlus](#) | Full Text: [PDF\(1549 KB\)](#) IEEE CFP



[Help](#) [Contact Us](#) [Privacy & Terms](#)
© Copyright 2006 IEEE. All rights reserved.